## **SYSLOG-2**

syslog() is subject to format string vulnerabilities.

Sean Barnum, Cigital, Inc. [vita<sup>1</sup>]

Copyright © 2007 Cigital, Inc.

2007-04-23

## Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 3619 bytes

Attack Category	Malicious Ir	Malicious Input				
Vulnerability Category	Format string					
	Buffer Overflow					
	• Unconditional					
Software Context	• Logging					
Location						
Description	syslog() is subject	syslog() is subject to format string vulnerabilities.				
APIs	<b>Function Name</b>	Commo	Comments			
	syslog					
	vsyslog					
Method of Attack	Use of syslog() can introduce vulnerability to a format-string attack.					
	syslog() is used to log system message. syslog() accepts a printf-style format string as a parameter for it's messages. Because of this, an attacker could potentially send a message that could cause syslogial.					
Exception Criteria						
Solutions	Solution Applicability	Solution Description	Solution Efficacy			
	When syslog is used.	Verify that input is of a limited size. If the message is coming from an outside source, check for %s type parameters and ensure that bounds will not be overwritten. Don't use text from an outside	Effective.			

<sup>1.</sup> http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

SYSLOG-2

		ource as a format string.		
Signature Details	void syslog( int priority, char *format,)			
Examples of Incorrect Code	[] openlog("my_program", 0, LOG_USER); void syslog( LOG_WARNING, textAHackerCouldInfluence); closelog(); []			
<b>Examples of Corrected Code</b>	[] openlog("my_program", 0, LOG_USER);			
	<pre>/* Truncate text to ensure not too big. If syslog() formatting supports it, could alternatively use formatting options that limit output size. */ char textBuffer[MAX_SAFE_TEXT_SIZE]; / * Safe size depends on syslog() implementation */ strncpy(textBuffer,textAHackerCouldIntextBuffer[sizeof(textBuffer)-1] = '\0';</pre>			Influence
	<pre>void syslog( textBuffer); closelog(); []</pre>	LOG_WARNING	G, "%s",	
Source Reference	• Viega, John & McGraw, Gary. Building Secure Software: How to Avoid Security Problems the Right Way. Boston, MA: Addison-Wesley Professional, 2001, ISBN: 020172152X, p. 148.			
Recommended Resource	• Syslog man page <sup>2</sup>			
Discriminant Set	<b>Operating System</b>	• Win	ndows	
	Languages	• C	+	

## Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

SYSLOG-2

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about "Fair Use," contact Cigital at copyright@cigital.com<sup>1</sup>. The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content. mailto:copyright@cigital.com

SYSLOG-2 3